UNIVERSITY OF
ILLINOIS LIBRARY
AT URBANA-CHAMPAIGN

[redacted]

Il6N
no.675

Math

UIUCDCS-R-74-675

ON THE EVALUATION OF POWERS

by

Andrew Chi-Chih Yao

August 1974

DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN · URBANA, ILLINOIS

UIUCDCS-R-74-675

ON THE EVALUATION OF POWERS

by

Andrew Chi-Chih Yao

August 1974

Department of Computer Science
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

Research supported by NSF GJ-41538.

Digitized by the Internet Archive
in 2013

http://archive.org/details/onevaluationofpo675yaoa

1. Introduction

An addition chain (of length r) is a sequence of r+1 integers $a_0, a_1, a_2, \ldots, a_r$ such that (i) $a_0 = 1$ and (ii) for each i, $a_i = a_j + a_k$ for some $j \leq k < i$. It is well known [4] that, for any r and any set of integers $\{n_1, n_2, \ldots, n_p\}$, there exists an addition chain of length r which contains the values $n_1, n_2, \ldots, n_p$ if and only if there exists a procedure which, for any input x, computes $\{x^{n_1}, x^{n_2}, \ldots, x^{n_p}\}$ in r operations using only multiplications. A theorem by Brauer [1] [4] states that, for any n, there exists an addition chain of length[1] $\lg n + O(\lg n/\lg\lg n)$ which contains the value n. This then implies the existence of a corresponding procedure to compute x^n in $\lg n + O(\lg n/\lg\lg n)$ multiplications. Furthermore, it was shown by Erdös [2] [4] that the above result is nearly the best possible. In an open problem posed in Knuth [3], it is asked if there are fast procedures to compute $\{x^{n_1}, x^{n_2}, \ldots, x^{n_p}\}$ for $p \geq 2$. This problem cannot be solved by a direct extension of the technique used by Brauer in the proof of his theorem.

In this paper we show that, for any positive integers $n_1, n_2, \ldots, n_p$ there exists a procedure using only multiplications which, for any input x, computes $\{x^{n_1}, x^{n_2}, \ldots, x^{n_p}\}$ in $\lg N$ + constant × $\sum_{i=1}^{p} [\lg n_i/\lg\lg(n_i+2)]$ multiplications where $N = \max_i\{n_i\}$. This gives a solution to Knuth's problem and leads to a corresponding theorem on addition chains which generalizes Brauer's theorem mentioned earlier.

2. Definition

Let e_i, $1 \leq i \leq p$, and f_j, $1 \leq j \leq q$, be positive integers. We shall say that $\{x^{e_1}, \ldots, x^{e_p}\}$ is computable from $\{x^{f_1}, \ldots, x^{f_q}\}$ in r multiplications ($r \geq 0$) if there exists a set of r positive integers,

---

[1] lg is logarithm to the base 2.

$\{f_{q+1},\ldots,f_{q+r}\}$, such that

(i) for all $i = q+1,\ldots,q+r$,

$x^{f_i} = x^{f_j} \cdot x^{f_k}$ for some $j \leq k < i$.

(ii) $\{x^{e_1},\ldots,x^{e_p}\} \subset \{x^{f_1},\ldots,x^{f_{q+r}}\}$.

Since the exponents are additive when two powers of x are multiplied, the above definition corresponds to a natural generalization of the definition of addition chains (cf. Section 1). The exponents appearing in $\{x^{f_1},\ldots,x^{f_q}\}$ correspond to a set of numbers initially available in the chain, as opposed to a single number, 1, in the earlier definition.

3. The Computation of $\{x^{n_1},\ldots,x^{n_p}\}$

The following lemma is well-known [4].

Lemma 1 For any integer $i > 0$, $\{y^i\}$ is computable from $\{y\}$ in less than $2\lfloor \lg i \rfloor$ multiplications.

Proof Let the binary representation of i be

$$i = \sum_{j=1}^{v} b_j \cdot 2^j \tag{1}$$

where $v = \lfloor \lg i \rfloor$. Then,

$$y^i = \prod_{b_j=1} y^{2^j} . \tag{2}$$

Thus, we first compute $y^2, y^4, y^8, \ldots, y^{2^v}$ sequentially in v multiplications. Then we can compute y^i by equation (2) in no more than v-1 multiplications. The total number of multiplications is no greater than 2v-1. ☐

Theorem 2 For any integers m,n where $0 < m \leq n$, $\{x^m\}$ is computable from $\{x,x^2,x^4,x^8,\ldots,x^{2^{\lfloor \lg n \rfloor}}\}$ in less than $c \lg n/\lg\lg(n+2)$ multiplications for some constant c.

Proof Assume $n \geqq 4$. Define the following quantities:

$$k = \lceil (\lg \lg n)/2 \rceil \tag{3}$$

$$D = 2^k \tag{4}$$

$$t = \lfloor \log_D n \rfloor \tag{5}$$

Let the D-ary representation for m be

$$m = \sum_{j=0}^{t} a_j D^j \quad \text{where } 0 \leqq a_j \leqq D-1 \quad \text{for} \quad j = 0,1,\ldots,t. \tag{6}$$

We partition the set of integers $\{0,1,\ldots,t\}$ into D disjoint subsets $S(0),S(1),\ldots,S(D-1)$ by letting

$$S(i) = \{\ell | a_\ell = i\} \qquad \text{for } i = 0,1,\ldots,D-1.$$

It follows from (6) that

$$m = \sum_{i=1}^{D-1} i \cdot [\sum_{\ell \in S(i)} D^\ell] = \sum_{i=1}^{D-1} i \cdot m_i \tag{7}$$

where

$$m_i = \sum_{\ell \in S(i)} D^\ell \tag{8}$$

From (7) and (8), we obtain the following two equations:

$$x^{m_i} = \prod_{\ell \in S(i)} x^{D^\ell} \qquad \text{for } i = 1,2,\ldots,D-1 \tag{9}$$

$$x^m = \prod_{i=1}^{D-1} (x^{m_i})^i \tag{10}$$

Since all the x^{D^ℓ} in (9) are available in the set $\{x,x^2,x^4,x^8,\ldots,x^{2^{\lfloor \lg n \rfloor}}\}$, we can construct a procedure to compute x^m as follows:

Step 1: For $i = 1,2,\ldots,D-1$ do the following:

(a) Compute x^{m_i} from (9) in less than $|S(i)|$ multiplications.

(b) Compute $(x^{m_i})^i$ in less than $2\lfloor \lg i \rfloor$ multiplications (by Lemma 1).

Step 2: Compute x^m from (10) in D-2 multiplications.

Let M be the total number of multiplications in the above procedure. Then,

$$M < \sum_{i=1}^{D-1} (|S(i)| + 2\lfloor \lg i \rfloor) + D - 2$$

$$\leq \sum_{i=1}^{D-1} |S(i)| + 2(D-1)\lg(D-1) + D - 2 \tag{11}$$

Noting that the S(i)'s form a partition of the set $\{0,1,\ldots,t\}$, we obtain from (11) that,

$$M < t + 1 + 2(D-1)\lg(D-1) + D - 2 \tag{12}$$

(12), together with equations (3), (4) and (5), implies

$$M < 2(\lg n/\lg \lg n) + 1 + 4(\lg n)^{1/2} \lg \lg n + 2(\lg n)^{1/2} \quad . \tag{13}$$

It follows from (13) that there exists a constant c such that

$$M < c \lg n/\lg \lg (n+2) \tag{14}$$

Thus the theorem is true if $n \geqq 4$. Obviously we can choose c so that the theorem is also true for $n = 1,2,3$. □

Theorem 3 For any set of positive integers $\{n_1, n_2, \ldots, n_p\}$, $\{x^{n_1}, x^{n_2}, \ldots, x^{n_p}\}$ is computable from input $\{x\}$ in less than $\lg N + c \sum_{i=1}^{p} [\lg n_i/\lg \lg (n_i+2)]$ multiplications for some constant c, where $N = \max_i \{n_i\}$.

Corollary $\{x^{n_1},x^{n_2},\ldots,x^{n_p}\}$ is computable from $\{x\}$ in less than $\lg N + cp\lg N/\lg\lg(N+2)$ multiplications.

Proof of Theorem 3 and Corollary First we compute $\{x,x^2,x^4,x^8,\ldots,x^{2^{\lfloor \lg N\rfloor}}\}$ from input x in $\lfloor \lg N\rfloor$ multiplications. For each i, according to Theorem 2, x^{n_i} is computable from $\{x,x^2,x^4,\ldots,x^{2^{\lfloor \lg n_i\rfloor}}\}$ in $c\lg n_i/\lg\lg(n_i+2)$ multiplications, and also from $\{x,x^2,x^4,\ldots,x^{2^{\lfloor \lg N\rfloor}}\}$ in $c\lg N/\lg\lg(N+2)$ multiplications for some constant c. The theorem and corollary then follow immediately. □

In terms of addition chains, Theorem 3 and its corollary give the following generalization of Bauer's theorem [1] [4].

Theorem 4 For any positive integers $n_1,n_2,\ldots,n_p$, there exists an addition chain of length less than $\lg N + c\sum_{i=1}^{p}\lg n_i/\lg\lg(n_i+2)$ containing the values $n_1,n_2,\ldots,n_p$ for some constant c, where $N = \max_i\{n_i\}$.

Corollary For positive integers $n_1,n_2,\ldots,n_p$, there exists an addition chain of length less than $\lg N + cp\lg N/\lg\lg(N+2)$ containing $n_1,n_2,\ldots,n_p$.

4. Conclusion

We have shown that $\{x^{n_1},x^{n_2},\ldots,x^{n_p}\}$ can be computed in $\lg N + cp\lg N/\lg\lg(N+2)$ multiplications for input x where $N = \max_i\{n_i\}$ and c is a constant. On the other hand, it is well-known that to evaluate $\{x^{n_1},x^{n_2},\ldots,x^{n_p}\}$ by arithmetic operations, at least $\lg N$ operations are necessary. Thus, our procedures for evaluating $\{x^{n_1},x^{n_2},\ldots,x^{n_p}\}$ are nearly the best possible when $p \ll \lg\lg(N+2)$. It remains an interesting open problem to determine the complexity of computing $\{x^{n_1},x^{n_2},\ldots,x^{n_p}\}$ for general p.

References

[1] Brauer, A., Bull. AMS 45 (1939), pp. 736-739.

[2] Erdős, P., Acta Arithmetica 6 (1960), pp. 77-81.

[3] Knuth, D. E., The Art of Computer Programming, Vol. 2, Addison-Wesley, 1969, Section 4.6.3 Ex. 32.

[4] Knuth, D. E., The Art of Computer Programming, Vol. 2, Addison-Wesley, 1969, pp. 398-418.

BIBLIOGRAPHIC DATA SHEET	1. Report No. UIUCDCS-R-74-675	2.	3. Recipient's Accession No.

4. Title and Subtitle

ON THE EVALUATION OF POWERS

5. Report Date
August 1974

6.

7. Author(s)
Andrew Chi-Chih Yao

8. Performing Organization Rept. No.

9. Performing Organization Name and Address

Department of Computer Science
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

10. Project/Task/Work Unit No.

11. Contract/Grant No.
NSF GJ-41538

12. Sponsoring Organization Name and Address

National Science Foundation
Washington, D.C.

13. Type of Report & Period Covered

14.

15. Supplementary Notes

16. Abstracts

It is shown that for any set of positive integers $\{n_1, n_2, \ldots, n_p\}$, there exists a procedure which computes $\{x^{n_1}, x^{n_2}, \ldots, x^{n_p}\}$ for any input x in less than $\lg N + c \sum_{i=1}^{P} [\lg n_i / \lg \lg (n_i+2)]$ multiplications for some constant c, where $N = \max_i \{n_i\}$. This gives a solution to an open problem in Knuth [3] and generalizes Brauer's theorem on addition chains.

17. Key Words and Document Analysis. 17a. Descriptors

addition chains, Brauer's theorem

17b. Identifiers/Open-Ended Terms

17c. COSATI Field/Group

18. Availability Statement	19. Security Class (This Report) UNCLASSIFIED	21. No. of Pages
	20. Security Class (This Page UNCLASSIFIED	22. Price

FORM NTIS-35 (10-70)

USCOMM-DC 40329-P71

NOV 1 1974

FEB 20 [illegible]

BOUND BY
HM

UNIVERSITY OF ILLINOIS-URBANA
510.84 IL6R no. C002 no.674-676(1974
Use of Riccati equation in digital compu
3 0112 088401465